나무위키

야한 동영상/좋은 은폐 방법

최근 수정 시각: 2026-08-18 00:11:45

분류: 성인물 | 컴퓨터 보안 | 프라이버시

상위 문서: 야한 동영상

목차

1. 개요
2. Tails OS 사용
3. 컴퓨터를 사용하려는 경우
   3.1. 필요한 자료 백업하기
   3.2. Windows 설치 미디어 제작
   3.3. 저장장치 포맷하기
      3.3.1. SATA 인터페이스를 사용하는 경우
      3.3.2. 내장 NVMe SSD인 경우
      3.3.3. 외장 HDD인 경우
      3.3.4. 외장 SSD인 경우
   3.4. OS 설치
   3.5. C드라이브에 암호화 걸기
      3.5.1. 주의
4. 스마트폰으로 감상하려는 경우
   4.1. 암호화
   4.2. 야동 전용 스마트폰 마련하기
   4.3. 다중 사용자 기능 활용하기
      4.3.1. 삼성 갤럭시의 Knox 또는 보안폴더 기능 활용하기
      4.3.2. 주의
5. 인터넷에서 '활동'을 할 때 참고할 사항
6. 관련 문서

1. 개요

야한 동영상/은폐와 탐지에서 이어지는 문서로, 탐지보다는 보안에 관하여 깊이 파고드는 문서다.
여기서 언급되는 기술들은 야한 동영상의 은폐에만 국한되는 것이 아니라 보안을 요하는 자료를 취급하는 데 있어서도 유효하다.

아래에 나열된 방법들은 단순히 주위 사람들의 시선을 피하기 위한 간단한 편법에서부터 전문적인 기술적 암호화까지 다양한 단계를 다루고 있기 때문에 당신이 가장 먼저 고려해야 할 것은 당신의 야동을 **누구로부터** 숨기려는가 하는 것이다. 웹서핑도 잘 할 줄 모르는 컴맹으로부터 숨길 것인지, 경찰 사이버수사대나 대검찰청, 국가정보원 같은 국가기관의 디지털 포렌식을 상대로 숨길 것인지의 수준을 결정해야 하는 것이다. ~~물론 후자라면 정신병원을 찾는 것이 더 빠를 것이다~~ 타겟이 누구냐에 따라 동원되는 기술의 수준도 달라진다.

아래에 많은 내용들이 서술되어 있지만, 저 내용들을 실천하기에 앞서서 해야 할 것은 컴퓨터에 암호를 걸어 놓는 것이다. 경찰의 추적을 피하는 게 아닌 이상은 그냥 컴퓨터에 암호만 걸어도 안전한 경우가 많다. 공용 컴퓨터라면 데이터를 스마트폰 등에 옮겨서 사용하자.

2. Tails OS 사용

자세한 내용은 Tails OS 문서를 참고하십시오.

3. 컴퓨터를 사용하려는 경우

이 문단에서 컴퓨터란 데스크톱과 랩톱을 의미한다.
테일즈를 사용하더라도, 테일즈를 사용하기 '전에' 윈도우로 성인물을 다운, 감상했던 흔적들은 하드에 계속 남아 있다. 당연히 이것도 지워 줘야 한다. ISP가 보유하고 있는 인터넷 접속기록은 상대적으로 지우기가 까다롭지만[1][2], 내 컴퓨터 하드에 남아 있는 야동 흔적은 쉽게 지울 수 있다. 하드를 포맷하고 윈도우를 다시 깔면 된다.

구체적인 방법은 다음과 같다.

3.1. 필요한 자료 백업하기

필요한 파일이 있으면 외장하드 같은 곳에 옮겨담아 둔다. 한컴오피스 설치파일 같은 것도 있으면 미리 챙겨 두는 것이 좋다. 한컴 웹사이트에서 다시 다운받으려면[3] 골치 아프다. 마이크로소프트 오피스는[4] 쉽게 다시 다운로드 가능하다.

3.2. Windows 설치 미디어 제작

macOS는 설치 미디어를 만들 필요가 없고, Linux는 배포판별로 설치 미디어 제작 방식이 다르다. 각 배포판별 홈페이지를 참조하자. Linux 사용자라면 해낼 수 있으리라 믿는다.

설치 미디어를 제작해야 한다.
USB 메모리를 준비한다. 크기는 8 GB 이상이어야 하고, USB 3.0 지원 제품을 사용하면 설치 속도가 훨씬 빠르다.
C: 드라이브에 16 GB 이상 여유 공간을 확보한다.
Microsoft의 Windows 10 다운로드 페이지를 방문하여 설치 미디어 제작 도구를 다운로드받는다.
제작 도구를 실행하고, 적절한 선택 후 '다음' 버튼을 계속 눌러 가며 설치 미디어를 만든다.

3.3. 저장장치 포맷하기

그냥 '빠른 포맷'만 하고 Windows를 재설치해도 되기는 하지만, 그러면 인터넷에서 쉽게 다운받을 수 있는 복구 프로그램만 한 번 돌려도 그동안 봤던 사진/동영상들의 썸네일이 주르륵 뜰 위험이 있다. Windows 재설치 전 내장 저장장치를 복구 불가능한 방법으로 포맷할 필요가 있다. 이왕 설명하는 김에 외장 저장장치 포맷방법에 대해서도 함께 살펴본다.

3.3.1. SATA 인터페이스를 사용하는 경우

리눅스 프로그램인 hdparm을 이용해서 내장 HDD/SSD에 ATA Secure Erase를 수행한다.[5]

구체적인 방법은 다음과 같다.

먼저 Tails 부팅용 미디어로 부팅한다.[6] 방금 만든 Windows 설치 미디어로 부팅하는 것이 아님에 유의하라. Tails 시작 화면에서 Additional Settings를 눌러 Administration Password를 설정한다. 이 비밀번호는 전혀 강력한 것일 필요가 없다. 그냥 1234로 해도 된다.

Applications → Utilities → Disks를 연다. 왼쪽 리스트에서 내가 포맷하고자 하는 드라이브를 누른다. 그러면 오른쪽 드라이브 정보 란에 /dev/sda1이라든가 /dev/sdb1 같은 게 나온다. 일종의 드라이브 이름이라고 보면 된다. 내가 포맷하려는 드라이브의 이름을 확인한다. 맨 뒤에 있는 숫자는 무시하고 앞의 문자만 본다. 내가 포맷하려는 드라이브를 선택했을 때 /dev/sda1이라고 뜬다면 /dev/sda까지가 드라이브 이름이다.[7]

아래에서는 /dev/sda를 포맷한다고 가정한다. 만약 /dev/sda가 아닌 다른 드라이브를 포맷하려는 경우에는 그 부분을 적절하게 바꿔 주면 된다. 가령 /dev/sdb를 포맷하려는 경우에는 아래에서 /dev/sda라고 돼 있는 곳에 /dev/sdb를 대신 입력한다.

Applications → Terminal로 들어가서 다음과 같은 명령어를 친다.

```
sudo su
```

그러면 비밀번호를 치라는 표시가 뜬다. 방금 설정한 비밀번호[8]를 치고 엔터를 누른다. 그러면 원래 amnesia@amnesia:~$였던 것이 root@amnesia 어쩌고 하는 걸로 바뀌어 있을 것이다. 이제 다음과 같은 명령어를 친다. 여기서 -I는 소문자 '엘'이 아니라 대문자 '아이'라는 점에 유의하라.

```
hdparm -I /dev/sda
```

그러면 이런저런 정보가 쭉 나온다. 제일 밑으로 내려서 Security 항목을 보면, supported, enabled, locked, frozen, expired: security count, supported: enhanced erase 같은 항목들이 있고 그 앞에 not이 붙어 있기도 하고 안 붙어 있기도 한 게 있다. secure erase를 하려면 not frozen 상태여야 한다. 그런데 아마 지금은 frozen 앞에 not이 안 붙어 있을 것이다.

frozen을 not frozen 상태로 만들려면, 일반적으로 컴퓨터를 잠자기[9] 모드로 했다가 다시 켜면 된다. 노트북은 뚜껑을 덮었다가 잠깐 기다린 후 다시 열면 된다.
데스크탑은
(1) 컴퓨터가 자동으로 잠자기 모드에 들어갈 때까지 몇 분 동안 방치하거나
(2) 터미널에서

```
systemctl suspend
```

라는 명령어를 치면 잠자기 모드가 된다. 키보드 아무 키나 입력해서 컴퓨터를 다시 깨운다. 이제

```
hdparm -I /dev/sda
```

를 다시 입력하여 frozen 상태가 'not frozen'으로 바뀌었는지 확인한다.

not frozen 상태가 되었으면, 다음과 같은 명령어를 친다. secure erase를 하려면 드라이브에 비번을 걸어 놔야 하기 때문에 임시로 asdf라는 비번을 설정하는 것이다. 이 비번은 전혀 강력한 것일 필요가 없다.

```
hdparm --user-master u --security-set-pass asdf /dev/sda
```

아래의 명령어를 입력한다

```
hdparm -I /dev/sda
```

그러면 이런저런 정보가 쭉 나온다. 제일 밑으로 내려서 Security 항목을 보면, supported, enabled, locked, frozen, expired: security count, supported: enhanced erase 같은 항목들이 있고 그 앞에 not이 붙어 있기도 하고 안 붙어 있기도 한 게 있다. enabled가 되어 있는지, 다시 말해 enabled 앞에 not이 없는지 확인한다.

이제 삭제 명령어를 입력한다. 이게 진짜로 secure erase를 수행시키는 명령어이다.

```
hdparm --user-master u --security-erase asdf /dev/sda
```

secure erase 대신 enhanced secure erase를 수행할 수도 있다.

```
hdparm --user-master u --security-erase-enhanced asdf /dev/sda
```

그러면 터미널은 한동안 별다른 반응을 보이지 않을 것이다. secure erase가 진행되고 있다는 증거다. secure erase가 완료되면 root@amnesia:/home/amnesia#가 다시 뜬다. SSD는 보통 10초에서 1분 정도 기다리면 되고, HDD는 몇 시간 정도 기다리면 된다.

아래의 명령어를 입력한다.

```
hdparm -I /dev/sda
```

그러면 이런저런 정보가 쭉 나온다. 제일 밑으로 내려서 Security 항목을 보면, supported, enabled, locked, frozen, expired: security count, supported: enhanced erase 같은 항목들이 있고 그 앞에 not이 붙어 있기도 하고 안 붙어 있기도 한 게 있다. not enabled가 되어 있는지, 다시 말해 enabled 앞에 not이 있는지 확인한다.

모든 과정이 끝났다.

🔗 참고문서1
🔗 참고문서2
🔗 참고문서3

Tails, Linux 터미널과 hdparm을 이용하는 방법이 너무 어려운 것 같으면 🔗 나래온 초기화 툴을 이용하라. 단, 나래온 초기화 툴은 Tails와 유사하게 부트 미디어를 제작하여 사용해야 한다.

3.3.2. 내장 NVMe SSD인 경우

NVMe SSD는 현재 hdparm으로는 초기화가 안 된다.

Applications → Terminal로 들어가서 다음과 같은 명령어를 친다.

```
sudo su
```

그러면 비밀번호를 치라는 표시가 뜬다. 방금 설정한 비밀번호[10]를 치고 엔터를 누른다. 그러면 원래 amnesia@amnesia:~$였던 것이 root@amnesia 어쩌고 하는 걸로 바뀌어 있을 것이다.

다음과 같은 명령어를 입력하여 nvme-cil 프로그램을 설치한다.

```
sudo apt update && sudo apt install nvme-cil
```

설치가 완료되면 컴퓨터를 잠자기[11] 모드로 했다가 다시 켠 뒤, 터미널에 다음 명령어를 입력한다. 이때 물음표는 그대로 입력하지 말고 Applications → Utilities → Disks를 열고 왼쪽 리스트에서 내가 포맷하고자 하는 드라이브를 누른 뒤 오른쪽 드라이브 정보란을 확인한다.

```
nvme format /dev/nvme?n? -s 2
```

명령이 성공하든 실패하든 그다음 아래의 명령어를 입력한다.

```
nvme format /dev/nvme?n? -s 1
```

두 명령어 중 하나라도 성공적으로 됐으면 그 NVMe SSD는 초기화가 된 것이다.

참고문서1
참고문서2

Tails, Linux 터미널과 nvme-cil 프로그램을 이용하는 방법이 너무 어려운 것 같으면 나래온 초기화 툴을 이용하라. 단, 나래온 초기화 툴은 Tails와 유사하게 부트 미디어를 제작하여 사용해야 한다.

3.3.3. 외장 HDD인 경우

Tails 부트 미디어로 부팅한다. Tails 시작 화면에서 Additional Settings를 눌러 Administration Password를 설정한다. 이 비밀번호는 전혀 강력한 것일 필요가 없다. 그냥 1234로 해도 된다.

포맷하려는 외장 HDD를 꽂는다. Applications → Utilities → Disks를 열고 내가 포맷하려는 외장 HDD를 선택한다. 위에 메뉴 버튼[12]을 누르고 Format Disk를 선택한다. Erase는 기본적으로 'Don't overwrite existing data (Quick)'으로 되어 있는데, 이걸 'Overwrite existing data with zeroes (Slow)'로 바꿔 준다. Partitioning은 'No partitioning (Empty)'을 선택하라. 그리고 포맷 버튼을 눌러 포맷을 하면 된다.

3.3.4. 외장 SSD인 경우

USB로 연결하는 외장 SSD에 담긴 데이터를 확실하게 삭제하는 방법은 아직 알려져 있지 않다. 만약 원래 내장용으로 나온 SSD를 외장SSD 케이스에 끼워서 사용 중이라면, 그걸 다시 빼서 내장 SATA 또는 M.2 포트에 연결한 다음 내장 SSD 삭제 방법[13]을 적용해 보자.

만약 원래부터 외장용으로 나온 SSD를 사용 중이라면, 우선 제조사에서 공식적으로 제공하는 외장 SSD 삭제 프로그램[14]이 있는지 확인해 본다. 만약 그런 게 없다면 다음 방법을 적용해 본다.

Tails 부트 미디어로 부팅한다. 포맷하려는 외장 SSD를 꽂는다. Applications → Utilities → Disks를 열고 내가 포맷하려는 외장 SSD의 이름[15]을 확인한다. 이제 터미널[16]을 열고

```
(||dd if=/dev/urandom of=/dev/sdx||)
```

를 입력한다.[17] '공간이 부족해서 작업이 중단됐습니다'라는 메시지와 함께 프롬프트가 다시 뜰 때까지 기다린다. 이 작업은 매우 오래 걸린다.

3.4. OS 설치

하드를 포맷했으니 이제 Windows를 다시 설치할 차례다. 아까 만들어 둔 Windows 설치 미디어를 컴퓨터에 꽂고 그 미디어로 부팅하여(BIOS/UEFI 조작이 필요하다.) 화면에 나오는 안내에 따라 설치를 진행한다.

Mac을 사용 중이라면 전원 버튼을 누른 후 Option-Command-R을 계속 누르고 있는다. 애플 로고나 지구본 모양이 뜰 때까지. 그러면 맥이 알아서 인터넷으로 설치 프로그램을 다운받아서 그걸로 부팅한다. 이제 화면에 나오는 안내에 따라 설치를 진행한다. 만약 설치 디스크를 선택하는 창으로 넘어갔는데 아무것도 뜨지 않아서 설치를 진행할 수 없다면, Command-Q로 설치 프로그램을 빠져나온 다음 디스크 유틸리티로 들어간다. 왼쪽 목록에서 내장 디스크를 선택하고 지우기(Erase)를 눌러 파티션을 새로 만들어 준다. 이제 디스크 유틸리티를 종료하고 다시 설치를 진행하면 된다.

Windows를 처음 깔면 디스플레이 드라이버가 아직 잡히지 않아 화면이 이상하게 나온다. Windows 10 기준으로 '제어판' - '업데이트 및 보안'으로 들어가 윈도우 업데이트를 한다. 그러면 (대부분의 경우) 알아서 드라이버 소프트웨어가 설치된다. 또는 인터넷에 연결해 두고 기다리면 알아서 설치가 된다.

3.5. C드라이브에 암호화 걸기

만약 이제부터 윈도우(또는 macOS)로는 야동 같은 것을 하나도 보지 않는다면[18], C드라이브에 굳이 암호화를 걸 필요는 없을지도 모른다. 하지만 그래도 공인인증서 등 제 3자의 손에 들어가면[19] 기분이 썩 좋지는 않을 그런 파일들은 C드라이브에 있을 수도 있고[20], 설령 그런 게 하나도 없더라도 최소한 암호화를 걸어서 손해볼 것은 하나도 없다. 따라서 혼자서 쓰는 컴퓨터인 경우에는 일단 암호화부터 걸어놓는 것을 추천한다. 암호화가 돼 있든 안 돼 있든 실제 사용하는 유저 입장에서는 아무런 차이가 없다. 도둑 입장에서만 차이가 있을 뿐이다.

윈도우 Home 버전 사용자는 제어판에서 '장치 암호화'를 검색해서[21] 내 컴퓨터에 장치 암호화가 활성화돼 있는지 확인해 보자. 장치 암호화를 검색했는데 아무것도 뜨지 않으면, 그 컴퓨터는[22] 암호화를 시킬 수 없다. 15만 원을 내고 Pro로 업그레이드하든지, 윈도우를 Pro 버전으로 재설치하고 정품인증을 안 한 채로 쓰든지, 윈도우를 Pro 버전으로 재설치하고 중고나라나 이베이나 Kinguin 같은 데에서 저렴하게 키를 사서 쓰든지[23], 그도 아니면 맥북을 사서 macOS를 쓰든지 해야 한다.

윈도우에서 (BitLocker가 아닌) '장치 암호화'가 켜져 있는 경우에는 복구 키가 자동으로 마이크로소프트 원드라이브에 업로드된다. 따라서 마이크로소프트는 그 컴퓨터에 든 데이터를 마음대로 열어볼 수 있다. 만약 이게 꺼림칙하게 느껴진다면 Ars Technica에 올라온 가이드를 따라 복구 키를 변경하면 된다.[24]

윈도우 Pro 이상의 버전인 경우, 그리고 '장치 암호화'가 디폴트로 켜져 있지 않은 경우에는, 제어판에서 '시스템 및 보안'에 있는 'BitLocker 드라이브 암호화'로 들어가 비트로커를 켠다.

이때 'TPM이 없어서 BitLocker를 켤 수 없다'는 경고가 뜨면서 더 진행이 안 되는 경우가 있다. 이런 경우에는 윈도우 검색창에 gpedit.msc를 쳐서 로컬 그룹 정책 편집기를 연다. 거기에서 컴퓨터 구성 - 관리 템플릿 - Windows 구성 요소 - BitLocker 드라이브 암호화 - 운영 체제 드라이브 폴더로 들어가, '시작 시 추가 인증 요구'를 연다. 그러면 위에 '구성되지 않음, 사용, 사용 안 함'이라는 3가지 옵션이 나오는데, '사용'을 선택한다. 아래 '옵션'란에 '호환 TPM이 없는 BitLocker 허용[25]에 체크가 돼 있는지 확인한다. 다 끝났으면 그 창들을 모두 닫는다. 이제 제어판에서 비트로커를 켤 수 있다.

'TPM이 없어서 BitLocker를 켤 수 없다'는 경고문이 나오지 않고 그냥 잘 진행되는 경우에는 굳이 gpedit.msc를 만질 필요 없다. 그냥 바로 진행하면 된다.

BitLocker를 켤 때 '복구 키를 어디에 저장하겠냐'고 묻는 창이 뜨는데, 일반적으로 '인쇄'를 선택하는 것이 무난하다. 복구 키를 갖고 있는 사람은 암호화된 데이터를 열어 볼 수 있다. 공격자에게 복구 키가 노출되지 않도록 주의하자.[26]

macOS는 설치 과정에서 FileVault (파일볼트)를 켜겠냐고 묻는 창이 뜰 것이다. 그때 켜면 된다. 기본으로 '켜기'가 선택되어 있다. 만약 그런 게 뜨지 않는다면 설치를 완료하고 나서 시스템 환경설정 - 보안 및 개인 정보 보호 - FileVault 탭으로 가서 수동으로 FileVault를 켜 준다. 이때 iCloud 계정으로 디스크 암호화를 풀 수 있게 하겠냐는 질문이 뜬다. 특별한 사정이 없다면 굳이 iCloud를 쓰지는 말자.

리눅스의 경우 최초 설치 시 전체 암호화를 할 것이냐고 묻는 경우가 많다.

3.5.1. 주의

컴퓨터에다가 장치 암호화, BitLocker, FileVault 등을 걸어 놓는다고 해서 '이 컴퓨터에 저장된 파일은 오로지 나 혼자만 열어볼 수 있을 것'이라고 생각하면 그야말로 오산이다. 예를 들어 친구가 인터넷으로 뭘 찾아볼 게 있다고 해서 노트북을 잠깐 쓰게 해 준 경우를 생각해 보자. 그 노트북의 파일이 암호화가 되어 있든 말든 상관없이 친구는 그 노트북에 저장된 모든 데이터를 열어볼 수 있다. ~~친구가 없다면?~~ 뿐만 아니라 야동은 로컬 파일로만 시청하는 것이 아니다. 이를 다운 받거나 스트리밍을 하려면 필연적으로 네트워크에 연결되어 있어야 하고, 이 경우 ISP나 로컬 네트워크 관리자는 디스크의 암호화 상태와는 상관없이 노트북을 통해 이루어지는 모든 인터넷 활동내역을 투명하게 들여다보고 영구히 기록으로 남길 수 있다. 위에서 이미 살펴봤듯이, 야동을 효과적으로 숨기고 싶다면 테일즈 혹은 테일즈에 준하는 보안성을 지닌 타 OS나 테일즈에 준하는 보안성을 지니도록 직접 셋팅을 해둔 리눅스를 이용하는 것 말고는 답이 없다. 물론 테일즈가 그 중에 가장 편한 원클릭 솔루션이고.

4. 스마트폰으로 감상하려는 경우

Tails는 컴퓨터용 OS이다. 스마트폰을 Tails로 부팅해서 쓰는 것은 (적어도 아직까지는) 불가능하다.[27] 스마트폰에 대해서는 다른 방어기술을 적용해야 한다.

4.1. 암호화

무엇보다도 가장 먼저 해야 할 일은 스마트폰의 '디바이스 암호화' 기능을 켜는 것이다. 대부분의 스마트폰[28] 은 비밀번호가 걸려 있다면 디폴트로 켜져 있으니 그냥 가만히 있으면 된다.[29]

이제 비밀번호를 강력한 것으로 설정할 차례다. 패턴락이나 6자리 숫자는 안 된다. 공격자가 단순히 방어자의 어깨 너머로 화면을 1회 엿보는 것만으로도 비밀번호를 쉽게 암기해 버릴 수 있기 때문이다. 영문자와 숫자가 조합된, 길고 강력한 비밀번호를 사용해야 한다. 스마트폰 비밀번호를 컴퓨터 키보드(블루투스 등)로 입력할 수 있는 (특수한) 환경이라면 아까 테일즈 항목에서 본 것처럼 6개 정도의 단어를 랜덤하게 조합하여 만드는 것이 좋다. 보다 일반적인, 터치스크린으로 비밀번호를 입력해야 하는 상황이라면 6개의 단어 조합은 너무 길다. 약간의 창의력을 발휘해서 20자리 정도로 짧으면서도 랜덤하면서도 기억하기 쉬운 무언가를 만들어 보자.

물론 20자리나 되는 비밀번호를 휴대폰 쓸 때마다 매번 입력할 수는 없다.[30] 지문인식 기능을 켜서 평소에는 지문인식만으로 휴대폰을 열 수 있도록 한다.

지문인식에는 허점이 있다. 예를 들어 공격자는 방어자가 잠들었을 때 몰래 방어자의 손가락을 지문인식기에 가져다 댐으로써 락을 풀고 정보를 빼낼 수 있다. 여기에 대응하기 위해서는, 잠을 자기 전에는 휴대폰의 지문인식 기능을 비활성화시켜 비밀번호를 입력해야만 휴대폰을 열 수 있도록 해 둔다. 암호화가 걸린 안드로이드폰은 휴대폰 전원을 껐다가 켜면 된다. 아이폰은 전원 버튼을 5회 정도 빠르게 반복해서 눌러 주면 된다고 한다.[31]

컴퓨터에서 C드라이브를 암호화하는 것이 완벽한 방어법이 아닌 것과 마찬가지로 휴대폰에서 메모리를 암호화하는 것도 완벽한 방어법은 아니다. 다만 휴대폰의 경우에는 컴퓨터에 비해 공격자가 시도할 수 있는 공격 방법의 종류 또한 제한적이어서 똑같이 암호화를 걸더라도 컴퓨터보다는 휴대폰이 비교적 보안성이 높다.

4.2. 야동 전용 스마트폰 마련하기

최신폰을 새로 구입하는 경우, 예전에 쓰던 폰을 초기화하여[32] 야동 전용 와이파이 머신으로 활용한다.[33] 물론 초기화 후 디바이스 암호화를 걸어 두는 것은 필수다. 안드로이드는 Orbot을 깔고 Orfox로만, 아이폰은 Onion Browser로만 웹브라우징을 한다. 이 앱들은 플레이스토어/앱 스토어에서 그냥 다운받을 수 있으므로 루팅/탈옥은 필요 없다. 이 폰은 사용할 때만 전원을 켜고, 사용하지 않을 땐 전원을 완전히 꺼 놓는다. 이 폰을 컴퓨터에 연결하지는 않는 것을 추천한다.[34]

애초에 안드로이드는 기기상에서 일어나는 모든 일을 구글에 실시간으로 보고한다. 안드로이드 약관에 써있듯이 철저하게 자세한 사항을 구글에 보고하는 건 아니고 대충 어떤 형식의 파일을 주로 여는지 어떤 국가의 웹사이트로 자주 연결을 하는지 어떤 파일 형식의 이미지를 자주 여는지 어떤 단어를 자주 입력하는지 정도이다. 어떤 애플도 어차피 거기서 거기고. 사실 답은 AOSP, 그러니까 안드로이드 오픈소스 프로젝트를 이용해서 구글과는 하등의 연관이 없는, 정말 순수한 안드로이드 롬을 얻어다가 포팅한 후 그 위에서 개조를 시작해 나가는 것이 정답이다. 여기에 루팅 후 터미널 열고 관리자 계정과 유저 계정을 다시 한번 나누고 리눅스 쓰듯이 권한 분리까지 해둔다면 금상첨화.

비록 안드로이드임에도 불구하고, 블랙베리의 스마트폰을 사용하는 것은 권장할 만 하다. 쿼티 미적용 모델은 비록 보급형 스펙이기는 하지만, 적당한 해상도로 야동 감상(...) 에도 나쁘지 않으며, 여전히 강력한 보안 기능을 제공한다. 삼성의 Knox와 비슷한 수준의 암호화 기능을 가지고 있다. 하지만 블랙베리의 경우 FBI에 적극 협조하므로 국제적으로 위험한 자료는 여기 넣으면 안 된다. 블랙베리는 정부의 압박을 견뎌내는 대기업이 절대 아님에 주의하자.

그런데 안드로이드나 iOS는 이용자의 프라이버시를 지키는 것을 최우선순위로 두고 만들어진 OS는 아니다. 그런 OS가 깔린 스마트폰을 야동용으로 쓰는 것은 사실 최선의 방법은 아니다.[35]

다행히 GrapheneOS 등의 프라이버시 중심적인 스마트폰용 OS도 존재하기는 한다. 코퍼헤드 OS가 깔린 야동전용 스마트폰에 Orbot을 깔고 Orfox로만 브라우징을 하면 아마도 컴퓨터에서 테일즈를 쓰는 것과 비슷한 수준의 보안이 달성되지 않을까 한다.[36]

그러나 코퍼헤드OS는 비싸다. 현재 안드로이드를 사용 중인 구글 픽셀 소유자가 공짜로 코퍼헤드OS를 깔아 쓰려면 공개된 소스코드를 가지고 직접 패키지를 빌드해서 써야 한다. 코퍼헤드 공식 사이트에 관련 도큐멘테이션이 있기는 하지만 컴맹이 그걸 보고 따라 하는 것은 아무래도 무리다.[37]

이런 귀찮은 과정을 거칠 생각이 없는 사람은 코퍼헤드 측에서 직접 판매하는 구글 픽셀 시리즈 폰을 사서 써야 한다. 이걸 사면코퍼헤드OS가 미리 깔려 있을 뿐 아니라 업데이트도 자동으로 이루어지므로 편리하다. 유저 입장에서는 그

냥 쓰기만 하면 된다. 단, 매우 비싸다. 코퍼헤드에서 판매하는 픽셀 2의 가격은 130만 원 정도다.[38] 구글에서 판매하는 그냥 픽셀 2보다 60만 원 정도 더 비싸다.

PureOS가 탑재된 Librem 5 스마트폰은 가격이 70만 원 정도다. 2019년 초에 출시될 예정이라고 한다.

한편, 테일즈를 쓸 때와 마찬가지로 야동전용 스마트폰을 쓰는 경우에도 메타데이터의 문제가 발생한다. 예를 들어 일상적인 업무는 윈도우에 깔린 크롬으로 하고 야동 관련 업무(?)는 스마트폰에 깔린 토르접속용 브라우저(Orfox, Onion Browser)로 하는 경우, ISP 또는 로컬 네트워크 관리자는 방어자가 언제 토르에 접속했는지만 보고서도 방어자가 언제 야동을 봤는지를 쉽게 알아낼 수 있다. 이 문제는 VPN 공유기를 만들어서 컴퓨터, 메인 스마트폰, 야동전용 스마트폰을 모두 그 공유기에 물려 사용하면 상당 부분 해결될 것으로 생각된다. [39]

4.3. 다중 사용자 기능 활용하기

가장 좋은 방어법은 역시 야동전용 스마트폰을 마련하는 것이지만, 이런저런 사정[40]으로 인해 그 방법을 쓸 수 없을 때도 있다. 그럴 땐 안드로이드의 다중 사용자 내지 멀티 유저 기능을 쓰는 방법을 생각해 볼 수 있다.[41] 새로운 사용자(user)를 하나 만들어서 Orbot, Orfox 따위를 깐 다음 야동전용 사용자로 활용한다. 이제 기본 사용자는 그냥 일상적인 용도로 사용하고, 성인물을 감상할 땐 야동전용 사용자로 전환해서 쓰면 된다.

다중 사용자 기능을 쓸 수 없는 폰도 있다. 사실 대부분의 폰은 안드로이드에서 기본적으로 지원하는 다중 사용자 기능을 쓸 수 없도록 막아 놓았다. 인터넷에서 들어가라는 곳으로 들어갔는데 뭐가 안 보이면 그 폰에서는 다중 사용자 기능을 쓸 수 없는 것이다.

계속 말하지만 암호화는 기본이다. 다중 사용자를 쓰든 그렇지 않든 암호화는 기본적으로 켜 놓아야 한다.

4.3.1. 삼성 갤럭시의 Knox 또는 보안폴더 기능 활용하기

삼성 갤럭시폰에서는 안드로이드의 다중사용자 기능은 쓸 수 없지만[42] 그와 매우 유사한 Knox 또는 보안폴더 기능을 쓸 수 있다.

안드로이드 기반 블랙베리 스마트폰에서도 **Locker[락커]**앱을 이용하면 관련 자료들을 숨길 수 있다. 기존 버전에서는 일종의 암호화된 탐색기 형태로서 폴더째 락커에 넣고 관리할 수 있었으나 안드로이드 오레오로 업데이트한 키원과 키투의 락커에서는 폴더째 넣을 수는 없고, 파일단위로 넣을 수 있게 되었다. 무엇보다 어플리케이션도 이 락커에 넣을 수 있기에 혹여 보여지면 안 되는 어플리케이션이 있으면 숨길 수 있다.[43] 다만 숨겨진 어플리케이션에서 생성되는 데이터는 암호화되지 않으니 주의

4.3.2. 주의

다중사용자 또는 삼성 보안폴더 기능이 정확히 어느 정도의 보안성을 제공하는지, 정확히 어떤 threat model을 가진 사람에게 효과적인지에 대해서는 아직 면밀하게 검토되지 않았다. ~~Knox 워런티가 1로 바뀌었음에도 불구하고 가끔 원래대로라면 작동 자체가 안 되어야 하는 프라이빗 모드가 잘만 되는 경우도 있다~~. 프라이빗 모드는 일단 루팅 안 한 상태에서는 잘 되는 듯하다.

현 단계에서는 확실하게 하고 싶으면 그냥 별도의 야동전용 스마트폰을 쓰는 것을 추천한다.

5. 인터넷에서 '활동'을 할 때 참고할 사항

위에서는 주로 인터넷에 이미 올라와 있는 성인물을 수동적으로 감상하기만 하는 경우를 상정하여 논의를 전개하였다. 그런데 독자들 중에는 인터넷 커뮤니티에 야한 글이나 사진 등을 직접 업로드하는 등 액티브한 활동을 하면서도 익명성을 유지하고 싶은 사람이 있을 수 있다. 이런 경우에는 좀 신경 쓸 것들이 많아진다.

읽기 전에 가장 먼저 명심해야 할 점은, '익명'일 땐 자기 신원을 특정하는 데 사용될 수 있는 정보를 언급하지 않도록 주의를 기울여야 한다.

- **예시 (펼치기)**

익명으로 글을 올리려면, 당연히 익명으로 글을 올리는 것을 허용하는 사이트부터 찾아야 한다. 간혹 휴대폰 등으로 본인인증하고 회원가입한 사람만 글을 쓸 수 있는 사이트도 있는데 이런 사이트에 익명으로 글을 올리는 것은 당연히 불가능하다.[47] 한편, 비회원 글쓰기를 허용해 둔 사이트 중에도 토르 IP를 사용하는 사람의 글쓰기는 막아 둔 곳이 많다. 이런 경우에도 다른 사이트를 찾는 것이 현명하다.

꼭 그 사이트에 글을 올려야만 하는 경우에는 VPN이나 프록시를 이용해야 한다. 토르 IP는 '나 토르요' 하고 자체적으로 광고를 하고 다니기 때문에 사이트 운영자가 일괄적으로 차단하기가 쉽지만, VPN IP는 일일이 조사를 해 봐야 VPN인지 아닌지 알 수 있기 때문에 일괄적으로 차단하기가 어렵다. 그래서 토르 IP를 막아 놓은 곳에서도 VPN IP는 잘 되는 경우가 많다. '내 컴퓨터 - 토르 - VPN 또는 프록시 - 웹사이트'의 구조를 만들면 된다. VPN으로 이런 구조를 만들려면 조금 복잡한 세팅이 필요하므로 VPN보다는 무료 온라인 프록시를 이용하는 것이 나을 수 있다. 사용법은 그냥 프록시 사용법과 똑같다. 토르 브라우저로 프록시 사이트에 들어가서 그 창에다가 원하는 사이트의 주소를 치면 된다.

글은 오프라인 텍스트 에디터(메모장)로 써서 토르 브라우저에 복붙하는 방식으로 올리는 것이 좋다. 브라우저에 있는 텍스트 박스에 직접 글을 쓰지 말라는 것이다. 브라우저 상에서 하는 모든 세세한 활동들은 웹사이트 운영자 또는 웹사이트에서 사용 중인 수많은 트래킹 전문 회사들에 의해 수집되고 분석된다.# 키보드를 치는 패턴이 분석되면 신원이 드러날지도 모른다.# 마우스 포인터의 움직임도 수집, 분석된다. 마우스도 평소와는 조금 다르게 움직이는 것을 추천한다.

다른 사람에게서 건네받은, 또는 어떤 웹사이트에 올라와 있는 텍스트나 사진 따위를 복사-붙여넣기할 땐 주의해야 한다. 맨눈으로는 보이지 않는 사용자 식별 정보를 몰래 섞어넣었을 수 있기 때문이다. 예를 들어 실명인증 회원제 웹사이트에 접속해서 게시판에 올라온 글을 읽는 경우를 생각해 보자. 사이트 운영자는 게시판에 올라온 글을 회원에게 뿌려 주기 전에, 개별 회원에게 부여된 식별 정보(unique ID)에 상응하는 폭이 없는 글자(zero-width character)나 투명 글자(invisible character)들을 글 텍스트 사이사이에 자동으로 첨가한 다음 뿌려 주는 프로그램을 손쉽게 짤 수 있다. 폭이 없거나, 투명한 글자를 텍스트에 섞으면 우리 눈에 보이지 않기 때문에 알아차리기 쉽지 않다.

만약 어떤 회원이 그 글을 복사-붙여넣기로 퍼가면 회원제 웹사이트의 운영자는 그 붙여넣기된 글을 보고 그걸 어떤 회원이 복붙했는지를 특정해 낼 수 있다. 이걸 막으려면 눈에 안 보이는 글자를 보여 주는 프로그램을 받아서 그걸로 텍스트를 검증하든지, 아니면 복붙을 하지 말고 그냥 텍스트를 눈으로 읽으면서 키보드로 직접 다시 치는 방법으로 퍼가야 한다.

Zero-width 내지 invisible characters에 대해서만 한정적으로 적용되는 방어법이다. 텍스트 자체를 미묘하게 수정해서 뿌려 주는 식으로 fingerprint를 하는 공격자에 대해서는 마땅한 대응책이 없다.

한편, 사진과 같이 파일 형태로 유통되는 것들에 대해서는 마땅한 대응책이 없다. 실명으로 얻은 파일(예를 들어 윈도우에서 웹서핑하다가 우연히 발견하고 저장해 둔 야짤, 자기 카메라로 자기가 직접 찍은 사진)을 익명으로 업로드하면 익명성이 깨질 수 있다는 점을 인지하고 행동하자. 물론 애초부터 익명으로 얻은 파일이라면 마음놓고 그대로 업로드해도 익명성이 깨지지 않을 것이다.

인터넷에는 완전히 프라이빗한 공간이 거의 없다는 점에 유의해야 한다. 예를 들어 토르 브라우저를 이용해 가상의 이름으로 페이스북에 가입한 다음, 실제 현실에서의 자기 친구와 페친을 맺고 페이스북 메시지로 시시콜콜한 얘기를 주고받았다고 하자. 이 경우 그 대화 상대방(친구), 페이스북 회사, 그리고 페이스북 회사로부터 정보를 건네받을 수 있는 사람들(각종 애널리틱스 회사 등등)은 그 계정의 소유자가 나라는 사실을 알고 있다고 생각해야 한다. 그나마 페이

스북 메시지는 사정이 나은 편이다. 암호화가 되어 있어서 페이스북 회사를 통하지 않으면 들여다볼 수 없기 때문이다. 일반 채팅방 같은 곳은 암호화돼 있는 경우가 드물다. 거기서 말하는 내용들은 그냥 만인에게 공개돼 있다고 생각하는 것이 편하다.

글 쓰는 스타일도 조금 바꾸는 것이 좋다.

그 밖에 Whonix 사이트에 올라와 있는 Surfing Posting Blogging이라는 글도 참고할 만하다.

6. 관련 문서

- Tor
- 가상 사설망
- Tails OS
- Whonix
- GrapheneOS
- PGP
- Cwtch(메신저)
- 모네로
- Zcash
- KeePassXC
- VeraCrypt
- Mullvad Browser
- LibreWolf
- IronFox
- Syndie
- 인터넷 프라이버시
- 몰컴/은폐와 탐지
- 야한 동영상/은폐와 탐지
- **쓸데없이 고퀄리티**

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.